IN THE DISTRICT COURT OF THE UNITED STATES
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
ASHEVILLE DIVISION

UNITED STATES OF AMERICA	)	
	)	**MEMORANDUM AND**
v.	)	**RECOMMENDATION**
	)	
CARL JACK HALL and	)	**1:16-CR-147**
MORRIS RYAN LITWACK,	)	**1:17-CR-60**
	)	
Defendants.	)	
	)	

Pending before the Court are Defendant Hall's Motion to Suppress and Dismiss, 1:16cr147 [# 18 & # 27] and Defendant Litwack's Motion to Suppress and Dismiss, 1:17cr60 [# 15]. The Government filed a Response in both cases, 1:16cr147 [# 22], 1:17cr60 [# 17]. The Court conducted a joint hearing and heard evidence and argument from the Government and Defendants. Defendants then filed Memorandums in Support of the Motions to Suppress and Dismiss, 1:16cr147 [# 33], 1:17cr60 [# 25]. The Government filed a Response to both Memorandums, 1:16cr147 [# 35], 1:17cr60 [#27]. Finally, the Government filed a Supplement to both Responses, 1:16cr147 [# 39], 1:17cv60 [# 32]. Having carefully considered the evidence, briefs, and arguments of counsel, the Court enters the following findings, conclusions, and recommendation.

FINDINGS AND CONCLUSIONS

I. Procedural Background

a. Carl Jack Hall, 1:16cr147

Defendant Hall is charged with receiving and possessing child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2)(A), 2252A(a)(5)(B). On April 25, 2017, Defendant Hall filed his Motion to Suppress and Dismiss [# 18]. On May 9, 2017, the Government filed its Response to Defendant Hall's Motion to Suppress [# 22]. On July 27, 2017, Defendant Hall filed a Supplement to the Motion to Dismiss [# 27]. On August 15, 2017, the Court held a joint hearing with the Government and Defendants Hall and Litwack. On September 19, 2017, Defendant Hall filed a Memorandum in Support of his Motion to Dismiss [# 33]. On September 29, 2017, the Government filed a Response to Defendant's Memorandum [# 35]. On November 13, 2017, the Government filed a Supplemental Response [# 39].

b. Morris Ryan Litwack, 1:17cr60

Defendant Litwack is charged with two counts of possessing child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). On June 15, 2017, Defendant Litwack filed his Motion to Suppress and Dismiss [# 15]. On June 22, 2017, the Government filed its Response to Defendant Litwack's Motion to Suppress [# 17]. On August 15, 2017, the Court held a joint hearing with the Government and Defendants Hall Litwack. On September 20, 2017, Defendant Litwack filed a

Memorandum in Support of his Motion to Dismiss [# 25]. On September 29, 2017, the Government filed a Response to Defendant's Memorandum [# 27]. On November 13, 2017, the Government filed a Supplemental Response [# 32].

In their Motions to Suppress and Dismiss, Defendants raise two arguments to suppress evidence or otherwise dismiss the cases against them: (1) the warrant from the Eastern District of Virginia, which led to the initial identification of defendants, was defective, overbroad, or void ab initio; and (2) the Government engaged in outrageous conduct.

II. Factual Background

a. Special Agent Daniel Alfin and Operation Pacifier

Defendants called FBI Special Agent Daniel Alfin as a witness. (T. 4)[1] Alfin was the case agent for Operation Pacifier. (T. 5) Operation Pacifier was an investigation into the child pornography website Playpen. (T. 5–6) Created in approximately in 2014, Playpen was hosted on The Onion Router (Tor) network. (T. 6). Tor is free computer software that cloaks users in anonymity. (T. 7–8) Six or seven volunteer computers, called nodes, bounce a user's internet connection potentially anywhere around the world. (T. 27) Thus, Tor users are free to browse the internet and create websites while remaining undetectable because the user does not leave an identifiable footprint. (T. 7–8, 27) The United States has no restrictions

[1] T. followed by a number is the page number of the transcript from the joint hearing held on August 15, 2017.

regarding access to the Tor network. (T. 9)

Initially, when Alfin discovered Playpen on the Tor network, there was little possible investigation due to Tor users' anonymity. (T. 11) While determining how to investigate Playpen, the FBI documented the content of the website. (T. 11) In December, 2014, the FBI caught a break. (T. 88) The FBI was able to locate the creator of the Playpen website due to a glitch that revealed the website creator's real Internet Protocol (IP) address. (T. 13–14) With the real IP address, the FBI was able to identify and prosecute Steven Chase as Playpen's creator. (T. 15)

On February 20, 2015, the FBI took administrative control over Playpen for thirteen days. (T. 18, 38) Prior to the takeover, however, Special Agent Douglas MacFarlane sought a search warrant from a magistrate judge in the Eastern District of Virginia. (T. 19–20) The FBI needed a warrant because even though it could take Playpen over, it still would not be able to identify individual Playpen users. (T. 17, 89) The FBI crafted a method that would allow it to identify individual users using a warrant and called it the Network Investigative Technique (NIT). (T. 19–20) The NIT warrant specified that the data to be collected included: (1) IP addresses; (2) a unique identifier generated by the NIT to establish the date the website was used; (3) the type of operating system used by the computer; (4) information about whether the NIT had already been delivered to the computer; (5) the computer's host name; (6) the computer's operating system username; and (7)

the computer's Media Access Control (MAC) addresses. [1:16cr147 # 18, Ex. 1 at 5] [hereinafter NIT Warrant]. With an IP address, the FBI can request the Internet Service Provider deliver identifying information, such as a home address, which is based on the IP address. (T. 97) A MAC address can narrow down the specific computer used in a household. (T. 99) Individual operating system information can identify a user's account on a computer looking up child pornography. (T. 99) Additionally, the FBI obtained a Title III intercept warrant that allowed the FBI to monitor private conversations between Playpen users who used the website's chat function. (T. 54)

In order for the FBI to obtain a user's identifying information, several steps needed to happen in order to trigger the NIT. (T. 30, 95) First, a user would have to find Playpen on the Tor network, either through an external link or via a website address consisting of sixteen random characters and ending ".onion". (T. 96) Second, a user had to log in to Playpen with a user name and password. (T. 30, 95–96) Third, a the user would need to navigate to a subsection of the website—Playpen had its subsections organized by content. (T. 30, 95–96) Fourth, a user would need to open a thread advertising child pornography from that subsection. (T. 30, 97) If the user downloaded content, that triggered the ability for the FBI to send hidden malware imbedded within the content. [NIT Warrant at 24]. The malware would capture a user's identifying information and transmit it back to the FBI in Virginia.

Id. While other theoretical investigative techniques were available, none were likely to be realistically effective and would require a lot of time and money. (T. 117)

Once the NIT transmitted the identifying information to the FBI in Virginia, that information was given to local FBI field offices. (T. 132) The local FBI offices would begin an investigation and apply for subsequent warrants in their respective districts. (T. 132)

When the FBI took over Playpen, it was decided that the FBI would operate the website in the Eastern District of Virginia. (T. 20) When the FBI transferred the operation to Virginia, Playpen was taken offline for a couple of hours. (T. 22) Before taking Playpen back online, the FBI presented the NIT warrant to a magistrate in the Eastern District of Virginia. (T. 20–21) The Magistrate Judge was aware that the warrant would allow the capture of information and lead to subsequent prosecutions of individuals outside the district. (T. 20–21)

Additionally, once the FBI had seized Playpen, it transferred Playpen's content to the National Center for Missing and Exploited Children (NCMEC). (T. 25) NCMEC identifies victims of child pornography and sends out victim notification letters when investigations are ongoing. (T. 25) Further, NCMEC let the FBI know which photos had previously been identified for victim restitution. (T. 129)

During the thirteen days of FBI takeover, Playpen registered approximately

100,000 new accounts—though not necessarily new users. (T. 39, 63) From time to time, the original Playpen creator would purge inactive accounts. (T. 63) So while Playpen user accounts increased from 317,000 accounts to 417,000 accounts under FBI control, these raw numbers do not reflect necessarily the total real number of Playpen users during its operation. (T. 62–63) Agent Alfin testified that for a website like Playpen, 100,000 new user accounts in thirteen days was within the realm of normal activity. (T. 64) Both before and after FBI takeover, Playpen had approximately 50,000 unique visitors a week. (T. 79)

The only alteration the FBI made to Playpen before taking it over was to remove a section of the website called "Producer's Pen." (T. 23) This was an area of the website that encouraged users to create new amateur child pornography. (T. 23, 37) To assuage any distrust by Playpen users, the FBI posted that the Producer's Pen section would soon be up and running again. (T. 36–37) Otherwise the website continued as it had before FBI takeover, including fluctuating website speed associated with the Tor network. (T. 25, 40–41, 70) Users remained free to upload and exchange content, including potentially new photos of victims. (T. 28) The FBI did not create new content. (T. 71) The FBI allowed Playpen to continue to function in this way because removing certain amounts or types of content can tip off users that the site is being investigated. (T. 28–29, 94) Agent Alfin testified that regarding consumers of child pornography, users of the Tor network are likely to be more tech

savvy compared to non-Tor users. (T. 87)

After thirteen days of FBI takeover, the FBI had identified approximately 8,000 individuals to investigate. (T. 46–47) While the FBI could have continued to operate Playpen, 8,000 new individual investigations, even spread among agencies, was determined to be a reasonable end point. (T. 47–48, 72) The FBI was keenly aware of the tightrope it walked in keeping users in the dark about the takeover. (T. 52) If a user was tipped off, he or she would likely destroy evidence (i.e., hard drive). (T. 84) Before taking down Playpen, the FBI posted to Playpen users that the site was going offline for an upgrade. (T. 85)

Project Pacifier has led to the worldwide prosecution of over 1,000 people and the rescue of over 200 victims of child sexual abuse. (T. 72, 103) The FBI continues to prosecute Playpen users from Project Pacifier. (T. 75)

b. The Eastern District of Virginia and The NIT Warrant

On February 20, 2015, Agent MacFarlane sought the NIT warrant from a magistrate siting in the Eastern District of Virginia. [NIT Warrant at 2]. The warrant was filed under seal and has been provided with redactions. Id. At that time, Playpen was located in the Eastern District of Virginia. Id. at 4. The warrant stated the places to be searched: activating computers. Id. A computer that operates the Tor network, accesses Playpen, and logs in with a username and password is an "activating computer." Id. Thus, in order for the NIT to be launched, the computer must first

log in to Playpen with a username and password. Id.

The warrant stated the information to be seized: (1) the activating computer's actual IP address along with the time and date of that determination; (2) a unique identifier generated by the NIT to distinguish date from one activating computer from that of another; (3) the type of operating system used by the computer; (4) information about whether the NIT had already been delivered to the activating computer; (5) the activating computer's host name; (6) the activating computer's operating system username; and (7) the activating computer's MAC addresses. Id. at 5.

The affidavit outlined the probable cause the FBI had in pursing the warrant. [NIT Warrant at 18]. In September, 2014, the FBI first became aware of Playpen. Id. Playpen's main page included "two partially clothes prepubescent females with their legs spread apart." Id. Underneath was text stating, "No cross-boards reposts, .7z preferred, encrypt filenames, include preview, Peace out." Id. Agent MacFarlane stated in his affidavit that these requests of users were tools of the trade for child pornographers. Id. The language represented the website's preferences, including file types and no repeat posts from other child pornography websites. Id. at 18–19. Additionally, once a user clicked the "register an account" hyperlink, Playpen offered a warning. Id. at 19. To access Playpen a user needed to input an email address. Id. The warning stated that a potential user should make a dummy

login email address and that users "should not post information here that can be used to identify you." Id. The affidavit went on to describe the sections and subsections of Playpen. Id. at 20–26. Then, the affidavit described how the NIT was to be employed. Id.

c. Defendant Hall, 1:16cr147

On March 1, 2015, Defendant Hall, under the username "amoura," accessed a post containing child pornography from Playpen, at which point the NIT was deployed to the activating computer. [1:16cr147 # 18 at 3]. The NIT collected Defendant Hall's information and sent it to the FBI in the Eastern District of Virginia. Id. Later that month, the FBI served an administrative subpoena on Charter to determine the user of the IP address transmitted to the FBI. Id. Charter identified Defendant Hall as the person receiving internet service at that IP address and provided Defendant Hall's Asheville home address. Id.

On July 13, 2015, local FBI obtained a residential search warrant from a magistrate in the district of Defendant Hall's residence, the Western District of North Carolina. [#18 at 3] On July 15, 2015, FBI agents executed the warrant on Hall's home, where they seized a Hewlett Packard laptop. Id. Later, the FBI found that the laptop had child pornography downloaded and the Tor network installed. Id. Defendant Hall was subsequently indicted for receiving and possessing child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2)(A), 2252A(a)(5)(B) [# 1].

d. Defendant Litwack, 1:17cr60

On October 11, 2014, Defendant Litwack, under the username "29stroke," first accessed the child pornography website Playpen. [1:17cr60 # 15 at 4]. After the FBI took over Playpen, Defendant Litwack again accessed child pornography at which point the NIT was deployed to the activating computer. Id. The NIT collected Defendant Litwack's information and sent it to the FBI in the Eastern District of Virginia. Id. Later, the FBI served an administrative subpoena on Charter to determine the user of the IP address transmitted to the FBI. Id. Charter identified Defendant Litwack's landlord as the person receiving internet service at that IP address and provided Defendant Litwack's Weaverville home address. Id.

Local FBI obtained a residential search warrant from a magistrate in the district of Defendant Litwack's residence, the Western District of North Carolina [# 15 at 4]. On December 17, 2015, FBI agents executed the warrant on Defendant Litwack's home, where they seized Litwack's desktop computer. Id. Later, the desktop computer would be found to have child pornography downloaded and the Tor network installed. Id. Defendant Litwack was subsequently indicted for two counts of possessing child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B) [# 1].

III. Discussion

a. The Warrant from the Eastern District of Virginia

i. Probable Cause, Particularity, and Scope

1. Legal Standards

> [N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularity describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV.

The standard of review for a magistrate's determination of probable cause is one of great deference. United States v. Blackwood, 913 F.2d 139, 142 (4th Cir. 1990). This review is further informed by the probable cause standard, which "is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." Illinois v. Gates, 462 U.S. 213, 232 (1983). Further, "[b]ecause of the fourth amendment's strong preference for searches conducted pursuant to warrants, reviewing courts must resist the temptation to "invalidate warrant[s] by interpreting affidavit[s] in a hypertechnical, rather than a commonsense, manner."" Blackwood, 913 F.2d at 142 (quoting Gates, 462 U.S. at 236). In reviewing a warrant application, the magistrate is required "simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him," including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, "there is a fair

probability that contraband or evidence of a crime will be found in a particular place." Gates, 462 U.S. at 238.

To that end, in reviewing a warrant application a magistrate may rely on law enforcement officers, who may "draw on their own experiences and specialized training to make inferences from and deductions about the cumulative information available to them that might well elude an untrained person," so long as the affidavit contains facts supporting the officer's determinations. United States v. Johnson, 599 F.3d 339, 343 (4th Cir. 2010) (quoting United States v. Arvizu, 534 U.S. 266, 273 (2002).

Regarding probable cause, anticipatory warrants are no different from ordinary warrants. United States v. Grubbs, 547 U.S. 90, 96 (2006).

> It must be true not only that if the triggering condition occurs there is a fair probability that contraband or evidence of a crime will be found in a particular place, but also that there is probable cause to believe the triggering condition will occur. The supporting affidavit must provide the magistrate with sufficient information to evaluate both aspects of the probable-cause determination.

Id. at 96–97 (internal quotations omitted).

In addition to the probable cause requirement, a warrant must contain with particularity "the place to be searched" and "the persons or things to be seized." United States v. Grubbs, 547 U.S. 90, 97 (2006). The place identified to be searched must be described with sufficient particularity "such that the officer with a search

warrant can, with reasonable effort, ascertain and identify the place intended." United States v. Owens, 848 F.2d 462, 463 (4th Cir. 1998) (quoting Steele v. United States, 267 U.S. 498, 503 (1925) (internal quotation marks omitted). Regarding the persons or items to be seized, nothing must be "left to the discretion of the officer executing the warrant" in deciding what to seize. Marron v. United States, 275 U.S. 192, 196 (1927).

The Fourth Amendment also limits the scope of a search. A search pursuant to a warrant is "limited in scope by the terms of the warrant's authorization." United States v. Williams, 592 F.3d 511, 519 (4th Cir. 2010) (quoting United States v. Phillips, 588 F.3d 218, 223 (4th Cir. 2009)). "[T]he scope of a lawful search is "defined by the object of the search and the places in which there is probable cause to believe that it may be found."" Maryland v. Garrison, 480 U.S. 79, 84 (1987) (quoting United States v. Ross, 456 U.S. 798, 824 (1982)). Thus, a court determines the valid scope of a search by looking at the relationship between the persons and items to be seized listed in the warrant and the likelihood that they will be found in the place to be searched.

2. Analysis

After reviewing the NIT warrant and affidavit, the Court finds that the warrant issued in the Eastern District of Virginia was supported by probable cause. Agent MacFarlane, a nineteen-year FBI veteran with specialized experience in child

pornography, gave the Magistrate Judge his affidavit and a warrant application. In the affidavit, Agent MacFarlane gave detailed probable cause to believe that anyone who entered Playpen was seeking to download or exchange child pornography.

The affidavit provided that for someone to access Playpen, first he or she would have to know about the dark web and download the Tor network in order to remain anonymous. Then, a user would have to find the Playpen web address, either through an existing user or via other child pornography discussion forums. The home page, as discussed above, left little to the imagination of what was behind the login page with images of two partially-clothed, prepubescent females. Thus, an innocent user would not stumble upon Playpen. Further, there were website rules on the homepage and a warning on the login page. The website rules, which appear as gibberish, were translated by Agent MacFarlane to show a preference for a compressed file type and that images were not to be reposts from other child porn websites. The warning on the login page advised users to create a fake email address and to protect their identities. After examining the totality of these circumstances, it is a fair probability to conclude that people accessing Playpen were doing so to trade and download child pornography. Therefore, the Court concludes that there was ample probable cause to support the NIT warrant.

Defendants argue that the warrant lacked particularity. To the contrary, the warrant outlined exactly the places to be searched: computers where someone logged

into Playpen by entering a username and password. The warrant also contained the seven specific items to be seized:

(1) the activating computer's actual IP address along with the time and date of that determination;

(2) a unique identifier generated by the NIT to distinguish date from one activating computer from that of another;

(3) the type of operating system used by the computer;

(4) information about whether the NIT had already been delivered to the activating computer;

(5) the activating computer's host name;

(6) the activating computer's operating system username; and

(7) the activating computer's Media Access Control.

Defendants contend that the NIT warrant allowed the FBI to search any computer. That is incorrect. The NIT warrant required that a user first log in to Playpen with a user name and password before the NIT could be deployed. In this case, logging in to Playpen serves as a sufficient trigger because of the fair probability that Playpen contained child pornography and that users who logged in would download and share such images.

Finally, the warrant was not overbroad. In particular, the likelihood was great that the identifying information to be seized would be on a Playpen user's computer.

ii. Federal Rule of Criminal Procedure 41(b) and § 636 of the Federal Magistrates Act

Defendants argue that the NIT warrant was unlawful because the issuing Magistrate Judge had no authority to issue a warrant to search any activating computer located outside the judge's district. Defendants argue that because this warrant was unlawful, evidence from the NIT and subsequent warrants must be suppressed.

Federal Rule of Criminal Procedure 41(b) and § 636 of the Federal Magistrates Act concern the scope of a magistrate's authority. Section 636 incorporates Federal Rule of Criminal Procedure 41(b). Other courts have analyzed the NIT warrant regarding Rule 41(b) with varied reasoning and outcomes. This Court, however, does not see the need for a Rule 41(b) analysis for two reasons. First, Rule 41(b) has been subsequently amended.[2] Second, the good faith exception first stated in United States v. Leon, 468 U.S. 897, 924 (1984), applies in this case.[3]

iii. Good Faith Exception

If a search violates the Fourth Amendment, "the fruits thereof are inadmissible under the exclusionary rule, a "judicially created remedy designed to safeguard the Fourth Amendment rights generally through its deterrent effect."" United States v.

[2] On December 1, 2016, an amendment to Rule 41(b) was adopted. This amendment clarifies that courts have venue to issue a warrant "to use remote access to search electronic storage media" inside or outside an issuing district if "the district where the media or information is located has been concealed through technological means." Fed. R. Crim. P. 41(b)(6)(A).

[3] See also United States v. Levin, 874 F.3d 316 (1st Cir. 2017); United States v. Horton, 863 F.3d 1041 (8th Cir. 2017); United States v. Workman, 863 F.3d 1313 (10th Cir. 2017) (determining that the good faith exception applies to other cases involving the FBI's NIT warrant).

Doyle, 650 F.3d 460, 466 (4th Cir. 2011) (quoting United States v. Calandra, 414 U.S. 338, 348 (1974)). Because exclusion is a severe remedy, it remains a "last resort." United States v. Stephens, 764 F.3d 327, 335 (4th Cir. 2014). In Leon, the Supreme Court first articulated a good-faith exception to the exclusionary rule. 468 U.S. at 922. Under Leon, a court is not required to exclude evidence obtained pursuant to a later-invalidated search warrant if law enforcement's reliance on the warrant was objectively reasonable. Doyle, 650 F.3d at 467.

The FBI agents' reliance on the NIT warrant was objectively reasonable, and it appears that the agents acted in good faith. A neutral and detached Magistrate Judge reviewed the warrant and determined that there existed probable cause to issue the NIT warrant. The FBI did not intentionally or recklessly mislead the Magistrate Judge in obtaining the NIT warrant. As discussed, the warrant contained ample probable cause to support the issuance of the warrant. The affidavit unambiguously described the places to be searched and the items to be seized. Finally, the FBI agents showed no improper conduct or misjudgment in relying upon the NIT warrant. Thus, the Leon good-faith exception applies in this case.

Therefore, the Court recommends that Defendants' motions to suppress evidence be denied.

b. Outrageous Government Conduct

i. Legal Standard

Defendants raise the Due Process claim that law enforcement conduct was "so outrageous as to violate fundamental notions of fairness." United States v. Hasan, 718 F.3d 338, 342 (4th Cir. 2013). While the existence of such a claim remains in theory, it has been "highly circumscribed." Id. at 343. See United States v. Russell, 411 U.S. 423, 431–32 (1973) (stating that there might arise a situation where police conduct is so outrageous that it would bar the government from "invoking judicial process to obtain a conviction."); Hampton v. United States, 425 U.S. 484, 490–91 (1976) (plurality opinion) (distinguishing the purpose of an outrageous police conduct claim from an entrapment defense and emphasizing that a Due Process Clause claim can only arise where government conduct violates a defendant's protected right); United States v. Goodwin, 854 F.2d 33, 37 (4th Cir. 1988) (finding that a due process violation only occurs where the government conduct was "outrageous, not simply offensive.")

In United States v. Hasan, 718 F.3d 338, 343 (4th Cir. 2013), the Fourth Circuit articulated the legal standard used by the Court for assessing a claim of outrageous police conduct:

> [T]he conduct must be shocking, or offensive to traditional notions of fundamental fairness.

Hasan. (internal quotations omitted). The threshold for this claim is high. United States v. Osborne, 935 F.2d 32, 36 (4th Cir. 1991); see United States v. Chase, ___ WL ___, 5:15cr15, at *2 (M.D.N.C. Sept. 6, 2016). See also United States v. Bogart,

783 F.2d 1428, 1438 (9th Cir. 1986) (outlining the outrageous government conduct standard and instructing the district court on remand to make findings of fact and complete a legal analysis regarding outrageous government conduct).

ii. Analysis

Defendants' claim of outrageous police conduct centers on the FBI takeover of the child pornography website Playpen. On February 20, 2017, the FBI took administrative control over Playpen for thirteen days. Before bringing the site back online, however, the FBI removed a section of the website that promoted the creation of new amateur child pornography. The FBI did not otherwise change the website—fearing it would tip off tech savvy users. The FBI did not create new child pornography. The FBI did not enhance, encourage, or contribute to the use of Playpen. The FBI waited for individuals to enter the website, navigate to a subsection, and download child pornography. In short, the FBI waited until a user clearly and by their own volition broke the law before acting. Then, the FBI employed the NIT to search an activating computer and seize the identifying information.

Defendants ask the Court to apply the reasoning in United States v. Twigg, 588 F.2d 373 (3d Cir. 1978). The Court, however, is not persuaded. In Twigg, the Government *supplied* laboratory materials and an "indispensable ingredient" for making "speed" to a defendant who might not have been able to acquire the materials

otherwise. Id. at 376, 380. Additionally, the Third Circuit found that the Government *encouraged* defendants, *provided* them technical skills, and *assisted* defendants when they had a problem committing the crime. Id. at 381. But for the Government's intimate involvement, defendants would not have committed a crime. Id. at 381. Here, the FBI did not provide Defendants with any materials that would help them access child pornography. The FBI did not create new child pornography for Defendants to download. The FBI did not encourage Defendants to download child pornography. The FBI did not provide any skills training to Defendants. The FBI did not have to assist Defendants because they had no technical problems downloading child pornography. Thus, this case is distinguishable from Twigg.

While the FBI operating a child pornography website might be unsavory, the FBI administrative takeover of Playpen, in this case, is not outrageous government conduct. It might have been a different analysis had the FBI created new child pornography, promoted the website, or otherwise helped users with Playpen. But the FBI did none of these.

Defendants also argue that by taking over the website, the FBI continued to harm child-pornography victims, which constitutes outrageous government conduct. This is unpersuasive for four reasons. First, as outlined above, the FBI did not create a new harm to victims. Rather, the FBI took administrative control over the already existing Playpen website and waited for Playpen users to break the law. Then, the

FBI would begin the process of investigation and prosecution of the lawbreakers. Again, the Court emphasizes that the FBI did not create a new harm to victims.

Second, the FBI, before and during the Playpen takeover, worked with NCMEC. The FBI supplied NCMEC with Playpen victims' photos. NCMEC would identify past victims, record new victims, and send out letters telling identified victims of the investigation. Thus, the FBI was aware of the sensitive nature of its investigation and worked with NCMEC to ensure that victims could be helped.

Third, Defendants base their claim on the protected rights of third parties—the victims. Defendants argue that Archer, 486 F.2d 670 (2d Cir. 1973), shows that "dismissal is . . . proper when government conduct causes injuries to innocent third parties" [1:16cr147, # 33 at 5]. In dicta, the Second Circuit did not endorse one way or the other that a defendant might be able to raise an outrageous government conduct claim based on harm to third parties. Archer, 486 F.2d at 677. Rather, that court was considering the outrageous government conduct analysis as a whole and mentioned the Government's position that it had not harmed a third party. Ultimately, the Second Circuit decided that case on other grounds. Thus, there is little precedent to persuade the Court that harm to third parties would allow a defendant to raise a claim of outrageous government conduct.

Finally, Defendants argue that the Court should weigh the interest of the FBI in its investigation versus the harm to the victims. Defendants characterize the FBI's

investigation as humiliating and endangering children. Operation Pacifier involved taking administrative control over an already existing website. The FBI waited until users broke the law by creating, transmitting, or downloading child pornography. Users were free not to view, download, or exchange child pornography. While other investigatory avenues were theoretically available, the NIT method was the best way—and perhaps the only way—because it allowed a large number of users to be identified, and it would not tip off users to destroy evidence. Other theoretical methods would not have been realistically effective. As mentioned above, the FBI's investigation into Playpen has led to numerous prosecutions and has helped save over 200 children worldwide. In this case, the FBI's interest in investigating and prosecuting those using child pornography outweighs the harm, if any, to victims.

Therefore, the Court finds that the FBI's conduct was not outrageous as to Defendants or to victims. The Court recommends that Defendants' motions for dismissal for outrageous government conduct be denied.

RECOMMENDATION

The Court respectfully **RECOMMENDS** that Defendants' Motions to Suppress and Dismiss, 1:16cr147 [# 18 & # 27] and 1:17cr60 [# 15], be **DENIED**.

Signed: December 7, 2017

Dennis L. Howell
United States Magistrate Judge

Timeline for Objections

The parties are hereby advised that, pursuant to Title 28, United States Code, Section 636(b)(1)(C), and Federal Rule of Civil Procedure 72(b)(2), written objections to the findings of fact, conclusions of law, and recommendation contained herein must be filed within fourteen (14) days of service of same. Responses to the objections must be filed within fourteen (14) days of service of the objections. Failure to file objections to this Memorandum and Recommendation with the presiding District Judge will preclude the parties from raising such objections on appeal. Thomas v. Arn, 474 U.S. 140, 140 (1985); United States v. Schronce, 727 F.2d 91, 94 (4th Cir. 1984).